Attachment 1

June 22, 1998

Executive Summary
Association Privacy Papers

The undersigned associations welcome the opportunity to engage in the public policy debate about privacy and the use of personal information. The members of the industries represented by these associations have a long history of successfully balancing the need for personal information to service their customers with the privacy concerns of those customers.

Moreover, each of these industries is subject to an extensive existing legal framework -- which may include constitutional and common law principles, federal and state statutes (both industry-specific and of general applicability), federal and state regulatory agency rules and self-regulatory organization (SRO) rules. These existing frameworks have successfully provided adequate consumer privacy protection heretofore and provide the means to address any future issues that may arise, while permitting the unobstructed flow of information that is vital to each of these industries and to the U.S. economy.

For instance, securities firms, investment companies and related entities are subject to a system of stringent regulation administered by the Securities and Exchange Commission (SEC) and SROs, such as the National Association of Securities Dealers. This system provides the framework to address any issues involving the protection of personal data. Similarly, insurance industry members are subject to an interwoven web of state, federal and common law standards that establish barriers against misuse of personal information and provide severe penalties for non-compliance. Financial institutions and their affiliates are regulated by federal and state banking agencies and other governmental entities, including state consumer finance administrators and the Federal Trade Commission. By enforcing federal and state statutes and regulations, these governmental entities ensure that the financial services industry appropriately protects the confidentiality of customer information. Financial institution customers also have long had common law privacy rights that have been enforced by courts across the U.S.

Furthermore, consumer confidence is the keystone of success within each of these industries. Simply put, it is in the self-interest of each industry's members to avoid misuse of private information. Each industry is subject not only to continuous government oversight, but also to close scrutiny by the media and the public. Particularly given the intensely competitive nature of these industries, no member could thrive -- or perhaps even survive -- for long should it gain a reputation for abusing confidential information. In fact, the protection of privacy is increasingly a product feature on which industry members compete. Consequently, voluntary practices that address customer privacy concerns, such as the establishment of privacy policies by individual companies, are developing rapidly and are continually evolving.

The unique, highly complex, and changing nature of privacy issues in each of these industries best lends itself to industry-specific solutions within the extensive, yet flexible, industry and regulatory regimes now in place. Rigid privacy standards of general application would stifle the flow of information, impose unnecessary costs and impede creative business innovations designed to benefit customers. Thus, the protection of privacy within these industries should not involve the creation of new regimes or mechanisms. Instead, privacy protection standards should be permitted to continue to evolve under the legal and regulatory regimes as they now exist.

Finally, these industries believe it would be improper, and severely detrimental to each industry and its members' customers, for the European Union (EU) or its member states to apply the EU Data Protection Directive in any way that denies industry members access to crucial data from EU customers and partners. Any disruption in the flow of information from the EU could, among other things, cause industry members to be unable to service accounts or process transactions for customers located abroad, and impede the ability of U.S. firms to acquire or form strategic alliances with EU firms. Moreover, in light of the existing laws, regulations and standards discussed above, the U.S. currently has a substantial network of privacy protections and the U.S. government should not respond to the EU Directive by imposing new requirements on industry members.

Privacy is a consumer concern, and therefore it is a concern of each industry member, who must win and keep consumers' trust. We do not need a one-size-fits-all regulatory scheme or a new bureaucracy to ensure that consumers can exercise informed choices about their privacy in each of these industry sectors. There are already market incentives and public referees to ensure that consumer's trust is honored.

American Bankers Association
Consumer Bankers Association
Securities Industry Association
Investment Company Institute
American Insurance Association
American Council of Life Insurance
Reinsurance Association of America
Insurance Services Office, Inc.
Alliance of American Insurers
The Council of Insurance Agents and Brokers
Independent Insurance Agents of America
International Insurance Council
Nat'l Association of Independent Insurers
Nat'l Association of Insurance Brokers
Nat'l Association of Mutual Insurance Companies
Professional Insurance Agents
MasterCard International Incorporated
Visa U.S.A. Inc.
Banking Industry Technology Secretariat
America's Community Bankers
Bankers Roundtable
Independent Bankers Association
National Retail Federation

Attachment 2

WILLIAM T. McCONNELL
PRESIDENT
Chairman and CEO
Park National Corp.
P.O. Box 3500
Newark, OH 43058-3500

November 13, 1997

TO: ABA Members

FROM: William T. McConnell
President, American Bankers Association

RE: JOINT INDUSTRY PRIVACY PRINCIPLES AND IMPLEMENTATION

Consumers around the world are becoming increasingly concerned about privacy issues related to financial and other personal data. With this consumer concern comes congressional, regulatory and media interest in ensuring that industries such as banking are protecting the personal and transactional information that has been entrusted to us. Our industry needs to show it is responding to these concerns. In addition, many individual ABA members have indicated they would like assistance in developing privacy principles for their institution. I am strongly encouraging each of you to formally adopt privacy principles similar to the attached. First some background:

- ABA established a Privacy Working Group (PWG) in response to a series of recommendations from ABA's Payment Systems Task Force, and that group developed industry guidelines for use by our membership. The PWG consulted with institutions of all sizes and received the ABA Board of Directors' formal endorsement earlier this year on eight general principles.

- ABA did not stop there, however, because we recognized that any industry response must be unified. Therefore, ABA met with the Bankers Roundtable, the Consumer Bankers Association and the Independent Bankers Association of America to agree on one set of principles. On September 18, before the House Banking Committee, ABA appeared with the other trade groups and formally released the privacy principles which I am attaching to this letter.

The Clinton Administration released a paper on privacy in electronic commerce in July and concluded that self-regulation was preferable to government mandates, but an inadequate response to consumer privacy concerns could result in regulation. ABA has learned that by the middle of 1998, the Department of Commerce will produce a report on private-sector efforts to ensure on-line privacy. Will the banking industry pass muster under

that review? We can succeed only if members produce specific privacy policies similar to what we issued in September.

NEED FOR ACTION

ABA has placed the attached privacy principles on its website (www.aba.com), and we are planning a telephone seminar on January 22, 1998, on tips for implementation. Our members feel strongly that each institution must develop its own method of implementation and enforcement, but keep in mind that there must be sanctions for violations of your bank's privacy policies or they will be seen as inadequate.

For now, we would recommend that in addition to enforceable policies, each institution should:

- Appoint a staff coordinator or committee in charge of privacy issues.
- Develop cross-institution training of all employees.
- Establish a method of monitoring for compliance.

In addition, as you will see from the principles, privacy policies are useless if the customer is unaware of what they are. Therefore, whether through the mail, by handouts in your institution or on your website, your privacy policies should be disclosed to the customer. ABA will continue to provide advice on how to use the privacy principles, but we would appreciate hearing from you on what procedures you are using. Please send your ideas, policies and tips to John Byrne at ABA, 1120 Connecticut Ave., N.W., Washington, D.C. 20036, or email jbyrne@aba.com.

Attachment (two pages)

PRIVACY PRINCIPLES

1. Recognition of a Customer's Expectation of Privacy

Financial institutions should recognize and respect the privacy expectations of their customers and explain principles of financial privacy to their customers in an appropriate fashion. This could be accomplished, for example, by making available privacy guidelines and/or providing a series of questions and answers about financial privacy to those customers.

2. Use, Collection and Retention of Customer Information

Financial institutions should collect, retain and use information about individual customers only where the institution reasonably believes it would be useful (and allowed by law) to administering that organization's business and to provide products, services and other opportunities to its customers.

3. Maintenance of Accurate Information

Financial institutions should establish procedures so that a customer's financial information is accurate, current and complete in accordance with reasonable commercial standards. Financial institutions should also respond to requests to correct inaccurate information in a timely manner.

4. Limiting Employee Access to Information

Financial institutions should limit employee access to personally identifiable information to those with a business reason for knowing such information. Financial institutions should educate their employees so that they will understand the importance of confidentiality and customer privacy. Financial institutions should also take appropriate disciplinary measures to enforce employee privacy responsibilities.

5. Protection of Information via Established Security Procedures

Financial institutions should maintain appropriate security standards and procedures regarding unauthorized access to customer information.

6. Restrictions on the Disclosure of Account Information

Financial institutions should not reveal specific information about customer accounts or other personally identifiable data to unaffiliated third parties for their independent use, except for the exchange of information with reputable information reporting agencies to maximize the accuracy and security of such information or in the performance of bona fide corporate due diligence, unless 1) the information is provided to help complete a customer

(continued)

initiated transaction; 2) the customer requests it; 3) the disclosure is required or allowed by law (*i.e.* subpoena, investigation of fraudulent activity, *etc.*); or 4) the customer has been informed about the possibility of such disclosure for marketing or similar purposes through a prior communication and is given the opportunity to decline (*i.e.* "opt out").

7. Maintaining Customer Privacy in Business Relationships with Third Parties

If personally identifiable customer information is provided to a third party, the financial institutions should insist that the third party adhere to similar privacy principles that provide for keeping such information confidential.

8. Disclosure of Privacy Principles to Customers

Financial institutions should devise methods of providing a customer with an understanding of their privacy policies. Customers that are concerned about financial privacy will want to know about an institution's treatment of this important issue. Each financial institution should create a method for making available its privacy policies.

# # #

PRIVATE ENTERPRISE

Virginia Dean, ABA Executive Director of Communications

Con men have sunk to new depths. It's called dumpster diving and it goes something like this: Crooks sift through banks' trash dumpsters — or other receptacles — in search of customers' names and account numbers which the thief's considerable desktop publishing skills then transform into fraudulent checks or documents.

On a related front, enterprising reporters, with visions of Pulitzers tap-dancing in their head, are turning the same trick, hoping to stumble upon confidential customer information and craft the find into a news story hot enough to etch their name in the annals of investigative journalism.

Whether it's the billions of dollars banks lose in check fraud each year or the blackening of bankers' image by the portrayal of them drop-kicking the public trust, the issue of dumpster diving should be taken seriously. Now.

Even though people routinely and serenely surrender credit cards worldwide to nameless waiters whom they couldn't pick out of a line-up 10 minutes later, concerns about privacy are growing. From the selling of mailing lists to the cloning of cellular phone numbers to evil-doers lurking on the Internet, people are getting justifiably nervous about the use of information about them without their permission.

Those mounting concerns, coupled with the wealth of proprietary information banks collect, present risks — and an opportunity.

Currently, there are no legal requirements on how banks should destroy customer records — or whether they should destroy them at all. But if history is any teacher, and if banks fail to safeguard customer records, a new layer of regulation will methodically be spread on the industry to see that they do so in the interest of consumers. Action now by banks can avoid both more regulation and the inevitable bad press. So what should they do?

- Have a specific plan for shredding (or otherwise destroying) documents.
- Make sure your employees understand the policy and why it's important.
- Make sure they follow it.

(And while you're at it, make sure all employees — the Oscar Madisons in the crowd as well as the Felix Ungers — don't leave confidential papers on their desk.)

Then tell your customers what the policy is. Tell them that you have a shredder (if you do) or an early-warning fraud alert system if activity on their account changes dramatically (if you do) or that you handle all transaction statements on your premises to ensure their security (if you do). Don't make them wonder what you're doing with their personal information. Let them know ***their*** privacy is one of ***your*** top priorities.

Advise them on how to protect their own interests. Urge them to destroy unused deposit slips and to tear up payroll stubs before they're put in the garbage. Nothing should go out that would give a crook the information he needs to commit fraud.

Imagine a story appearing in your local paper tomorrow, reporting the discovery of your customers' names and account numbers in your trash dumpster. It's an avoidable nightmare.

Internet mail: vdean@aba.com

Attachment 3

Consumer Alert
from the American Bankers Association

Identity Theft is on the Rise
You Can Protect Your Financial Identity

Identity theft is one of the fastest-growing types of financial fraud. Without stealing your wallet, a crook can steal your financial identity with as little information as your social security number. It is also called "account-takeover fraud" or "true-name fraud," and it involves crooks' assuming your identity by applying for credit, running up huge bills and stiffing creditors – all in your name.

Protect yourself by taking the following steps:

1. Get a copy of your credit report from each of the three major credit bureaus every year. It lists all of the lines of credit in your name. Check to be sure that everything is accurate, that all of the accounts are yours and that accounts you have requested to be closed are marked closed. Bureau reports cost around $8 each. But, if you've been turned down for credit, you are eligible for a free report.

   To order credit bureau reports, call:

Trans Union Credit Services	Equifax Credit Services	Experian Credit Services
800-888-4213	800-685-1111	888-397-3742

2. Keep an eye on your accounts throughout the year by reading your monthly/periodic statements thoroughly. That's an easy way for you to be sure that all of the activity in your accounts was initiated by you.

3. Tear up or shred pre-approved credit offers, receipts and other personal information that link your name to account numbers. Don't leave your ATM or credit card receipt in public trash cans. Crooks (a.k.a dumpster divers) are known to go through trash to get account numbers and other items that will give them just enough information to get credit in your name.

4. If your credit card or other bills are more than two weeks late, you should do three things: First, contact the Postal Service to see if someone has forwarded your mail to another address. Second, contact your bank to ask if the statement or card has been mailed. Third, contact the businesses that send you bills.

5. When you pay bills, don't put them in your mailbox with the red flag up. That's a flashing neon light telling crooks to grab your information. Use a locked mailbox or the post office.

6. Protect your account information. Don't write your personal identification number (PIN) on your ATM or debit card. Don't write your social security number or credit card account number on a check. Cover your hand when you are entering your PIN number at an ATM.

7. Don't carry your Social Security card, passport or birth certificate unless you need it that day. Take all but one or two credit cards out of your wallet, and keep a list at home of your account information and customer service telephone numbers. That way, if your wallet is lost or stolen, you'll only have to notify a few of your creditors and the information will be handy.

8. Never provide personal or credit card information over the phone, unless you initiated the call. Crooks are known to call with news that you've won a prize and all they need is your credit card number for verification. Don't fall for it. Remember the old saying, "if it sounds too good to be true, it probably is."

Take action if you are a victim:

1. Financial fraud is a crime; call the police.

2. Contact the fraud units of all three credit bureaus. Ask them to "flag" your account, which tells creditors that you are a victim of identity fraud. Also, add a victim's statement to each of your credit bureau reports that asks creditors to contact you in person to verify all applications made in your name.

3. Call the fraud units of the credit bureaus at:

Trans Union	Equifax Fraud	Experian Fraud
Fraud Assistance	Assistance	Assistance
Department	Department	Department
800-680-7289	800-525-6285	888-397-3742

4. Notify your banks. They can help you obtain new account numbers for all of your checking, savings and other accounts. Be sure to pick a new PIN number for your ATM and debit cards. Close all of your credit card accounts and open with new account numbers.

5. Notify the Postal Inspector if you suspect mail theft – a felony.

6. Depending on your situation, you may want to contact the Social Security Administration to get a new Social Security number. Their telephone number is 800-680-7289. You also may want to contact your telephone, long distance, water, gas and electrical companies to alert them that someone may try to open an account in your name.

7. Finally, make sure to maintain a log of all the contacts you make with authorities regarding the matter. Write down each person's name, title, and phone number in case you need to re-contact them or refer to them in future correspondence.

ABA FRAUD ALERT

Attention Customer Service Personnel: Bank customers trust banks to safeguard not only their money, but also confidential information about their accounts and finances. A relatively new fraud scheme, however, could threaten that all-important trust relationship. ABA provides the following information as a member service.

The Scheme: Certain unscrupulous private investigators or "information brokers" impersonate bank customers over the phone to get information such as account numbers or balances. The PIs use a variety of urgent reasons why they need the information. One example: *"I'm on my way out of the country and need to verify my balance so I have enough money to cover a check I'm writing."*

When is it legal or illegal to divulge information about a customer's account?

Check your bank's policies and procedures regarding disclosure of information. While it is legal to provide account balances or other information about an account *to the customer*, banks normally require customers to provide a photo ID (if face-to-face) or password and other private information (if over the telephone or via PC) to verify their identities.

It is illegal to knowingly divulge information about a customer's bank account to any third party, unless the information is requested via a subpoena or is for commercial purposes. Providing information to a third party without customer notice or consent violates a number of federal and state laws. Bank employees who release private information without prior customer consent risk penalties or legal action by their employer, the government or the customer whose information is disclosed.

Don't be a target

- Review your bank's security procedures. Make sure strict account-confirmation and privacy procedures exist.
- Demand that account inquiries be in writing, that is then verified, or via subpoena.
- Make sure all employees receive periodic training on security procedures.
- Know how to spot an impersonator.

Signs include: Someone without proper identification (if face-to-face); a caller becoming irate if an employee refuses to divulge information without proper identifying credentials; or the same person calling back several times to ask questions about an account. Banks with call-frequency tracking systems should monitor the frequency of callers inquiring about specific accounts.

Bank employees walk a fine line between good service and adequate security. It's possible that following bank policies closely could upset some customers. Bank employees should reassure these customers that the procedures are in place to protect all customers against fraud. Finally, employees who suspect fraud should immediately report it to the bank and law enforcement personnel.

www.aba.com

Attachment 5

NEWS

PUBLIC RELATIONS 1120 Connecticut Avenue, N.W., Washington, DC 20036 (202) 663-5000

Contact: John L. Hall
(202) 663-5473

FOR IMMEDIATE RELEASE

July 9, 1998

ABA STATEMENT ON SENATE MARKUP OF IDENTITY THEFT LEGISLATION

by Donald G. Ogilvie
Executive Vice President, ABA

"We fully support Senator Jon Kyl's identity theft bill that was marked up by the Senate Judiciary Committee today, and urge its prompt passage by the full Senate.

"By making identity theft a federal crime, consumers will have direct recourse against criminals who prey on individuals by stealing their personal information to commit financial fraud. Too many innocent people, and businesses such as banks, have become victims of identity theft and this bill will give prosecutors the necessary tools to hold those criminals responsible. This is a pro-privacy initiative that should be supported by the wide array of groups that are concerned about the abuse of sensitive information.

"Banks are working hard to educate consumers how to protect themselves from financial fraud and are reviewing and revising their own privacy policies to ensure that confidential customer information never leaves the bank. If Senate bill 512 becomes law, it will greatly assist the U.S. and the banking industry in our ongoing efforts to protect customer data."

###

The American Bankers Association brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks – makes ABA the largest banking trade association in the country.